MARTHA COAKLEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

Identity Theft: It Could Happen To You

Attorney General Martha Coakley's Guide to Protecting Yourself and Your Credit

January 2007

Where do identity thieves obtain personal information?

- Bank statements
- Discarded credit card and ATM receipts, trash dumpsters
- Pre-approved credit card applications
- Stolen mail
- Theft of a wallet or purse that contains credit cards, social security card, or driver's license
- Passport
- Unsecured Internet websites
- Sham telemarketing calls
- Sham emails and Internet websites
- Computer viruses and spyware
- Computer software found on public access computers or surreptitiously installed on home computers that log your keystrokes

Avoiding Identity Theft

Manage your personal information:

- Do not routinely carry your social security card or birth certificate in your wallet or purse. Carry only those credit cards you use regularly and cancel all credit cards you do not use.
- Keep an accurate list of all credit cards and bank accounts including the name, mailing address and telephone number of the creditor, the account number, and expiration date. Update the list regularly and keep it in a secure place.
- Review closely all credit card and bank statements each month to detect unusual activity or unauthorized charges.
- Destroy pre-approved credit card solicitations and reduce the number of those solicitations by calling 1 (888) 5-OPT-OUT (1-888-567-8688), or visit the website at www.optoutprescreen.com. Disclose your social security number only when absolutely necessary. Social Security numbers were implemented as a method to account for your taxable earnings, not as a universal identifier. Change your driver's license number to a randomly assigned "S number." When you pay by check, the seller can only record your name, address, driver's license or Massachusetts ID number, and your choice of a home

or daytime telephone number (M.G.L. c. 93, § 105). If you have a random license number, you avoid disclosing your Social Security number every time you pay by check.

- Don't give out any personal information on the telephone, through the mail, or over the Internet, unless you've initiated the contact or are sure you know with whom you are dealing.
- Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail promptly from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Office at 1- 800-275-8777, to ask for a vacation hold. Destroy all credit card and ATM receipts and do not discard them at banks or retail establishments.

Manage your computer:

- Update your virus protection software regularly. Computer viruses can have damaging effects, including introducing programs that cause your computer to send out files or other stored information.
- Update the security protections on your operating system by downloading any security updates or patches.
- Don't download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your computer or modem.
- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer.
- Use a secure browser. When you're submitting information on the Internet, look for the "lock" icon on the status bar. It's a symbol that your information is secure during transmission.
- Avoid using an automatic log-in feature that saves your username and password, and always log off when you're finished.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a password that is a combination of letters, numbers, and symbols.
- Don't respond to unsolicited emails that ask for personal information, even if it appears to come from a legitimate bank or other business. ID thieves will replicate emails and websites from legitimate companies, including banks and other financial institutions, to try to trick you into revealing your personal information. This tactic is called "phishing."

Order copies of your credit report from each of the three major credit bureaus (Equifax, Experian, and TransUnion).

- A credit report contains information such as where you work and live, all the credit accounts that have been opened/closed in your name, and whether you pay your bills on time. Check to see if you have authorized everything on your credit report.
- Under state and federal law, you are entitled to one free copy of your credit report each year from each of the three credit reporting agencies. You are also entitled to a free credit report when you request that a fraud alert be placed in your credit file, as described later in this document. Exercise this right, and check your credit report closely for accuracy.
- You can order your credit report by calling each of the three credit reporting agencies directly or you can order all three reports by contacting the centralized source: 1 (877) FACT-ACT (1-877-322-8228), or visit the website at www.annualcreditreport.com.

- In general, if you request more than one credit report each year, and you have not placed a fraud alert in your credit file, credit reporting agencies may charge you no more than $8.00 for a copy of your credit report.

Special considerations for individuals in the military:

- If you are on active military duty, consider placing an alert on your credit file. An alert will appear on your credit file for a 12-month period and special care must be taken before extending credit in your name. It also means that for two years from the date you make a request to have an active military duty alert placed on your credit file, credit bureaus must exclude you from any lists of consumers they provide to any third party to offer credit or insurance to you when you did not initiate the transaction.

What should you do if you are the victim of identity theft?

Take actions immediately to minimize damage to your credit record, and to ensure that you are not held responsible for debts which the identity thief incurred using your name.

Keep a record of all correspondence and conversations with financial institutions and other companies, credit bureaus, and law enforcement officials.

Send all correspondence by certified mail, return receipt requested, to document what the company received and when. Keep copies of everything.

You should take the following four steps in all instances of identity theft:

(1) **Close any problem accounts**.

Contact the credit card companies, banks, or any other creditors to close the accounts that you know have been tampered with or opened fraudulently.

(2) **Contact the credit bureaus and place a fraud alert on your credit file**.

Contact the fraud department of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requires that creditors contact you before opening any new accounts or making any changes to your existing accounts. When you place a fraud alert on your credit file, all three credit bureaus are required by law to automatically send a credit report free of charge to you. This "one-call" fraud alert will remain in your credit file for at least 90 days.

When you get your three credit reports, review them carefully. Look to see whether there are any accounts that you did not open, unexplained debts on your true accounts, and inquiries that you didn't initiate. Contact any companies if there is any unexplained activity. The three major credit bureaus are:

Equifax
P.O. Box 740241
Atlanta, GA 30374- 0241
To report fraud, call: (800) 525-6285

Experian
P.O. Box 2002
Allen, TX 75013
To report fraud, call: (888) 397-3742

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
To report fraud, call: (800) 680-7289

(3) **Contact the fraud departments of each of your creditors**.

If you are obtaining new accounts from your creditors, make sure to use new personal identification numbers (PINs) and passwords.

Make a list of all of the financial institutions where you do business, including your credit card companies and all of the financial institutions where you have checking, savings, investment, or other accounts. You should also identify your telephone, cell phone and Internet Service Providers. To make sure that each of your creditors is aware that an identity thief may have your account information, report to each of these companies that you have been the victim of identity theft, even if that particular company has not been the subject of the fraud. Ask each of your creditors to place a "fraud alert" on your account. It is a good idea to follow up in writing to each of the companies that you contact, and to keep a record of your letters.

Make phone calls today if your cards have been stolen. If your ATM or debit card has been stolen, even if you are unsure whether these cards have been used, report the thefts immediately to your bank or card issuer. If your credit cards have been stolen, also report these thefts immediately, whether or not you are aware that the cards have been used.

(4) **Promptly make a report with your local police department**.

File a police report with your local police department, keep a copy for yourself, and give a copy to your creditors and the credit bureaus.

Place an extended alert on your credit file. If you made an identity theft report to a police department, you may submit a copy of that report to one of the three major credit bureaus, and then an extended fraud alert will be placed in your credit file for a 7-year period. Having a fraud alert on your credit file means that any time a "user" of your credit report (for instance, a credit card company, lender, or other financial institution) checks your credit report, it will be notified that you do not authorize any new credit cards, any increase in credit limits, the issuance of a new card on an existing account, or other increases in credit, unless the "user" takes extra precautions to ensure that it is giving the additional credit to you (and not to the identity thief).

Massachusetts law provides that identity theft is a crime (M.G.L. c. 266, § 37E). You should be aware that not all identity theft complaints can or will be investigated. However, by providing law enforcement offices with a written report, you make it possible for law enforcement offices to spot trends and patterns, and to identify the prevalence of identity theft.

What's Next?

In general: Review all credit, billing, and bank statements with great care after you have been the victim of identity theft, and report all questionable activities to the appropriate company or financial institution.

Contact your bank if your checks have been stolen. You may learn that the identity thief has written checks in your name. If so, you need to alert your bank, and close your bank account. (Remember to discuss with your bank representative what to do about outstanding checks that have not yet been cashed.) Ask your bank to notify appropriate check verification services that you have been the victim of identity theft.

Many retail stores use check verification systems, and you can alert check verification systems about the identity theft, and ask them to stop accepting checks in your name drawn on the account you are closing.

The major check verification companies are:

Telecheck	(800) 710-9898	**ChexSystems**	(800) 428-9623
Certegy, Inc.	(800) 437-5120	**SCAN**	(800) 262-7771

Contact the Registry of Motor Vehicles if you need to get a new driver's license. If you were issued a driver's license by the Massachusetts Registry of Motor Vehicles, you may use the RMV's website for information about obtaining a new driver's license at www.mass.gov/rmv/.

Contact the U.S. Postal Inspection Service if you suspect that your address has been fraudulently changed. Notify the U.S. Postal Inspection Service if you suspect that an identity thief has filed a change of your address with the post office. You will also need to notify your local postmaster to make sure that all mail in your name comes to your address.

Contact the Passport Agency if your passport was stolen. If your passport was stolen, you need to take two steps:

(1) You should immediately report that your passport was stolen by completing a written form provided by the Passport Office.

(2) In order to get a new passport, you need to complete a form to replace a lost or stolen valid passport. To get instructions for obtaining and completing these forms, and to download the forms, visit the Passport Office's website at www.travel.state.gov.

Cell or telephone service. If you discover charges for calls you did not make on your cell or telephone bills, contact your provider immediately. You will probably need to close your accounts and open new ones. You may also want to request that a password be provided and required before any changes can be made to your accounts.

Identity Theft Resources

Attorney General Martha Coakley's Consumer Complaint and Information Hotline
(617) 727-8400

Federal Trade Commission
1 (877) 438-4338

EQUIFAX
1 (800) 525-6285 to request fraud investigation
1 (800) 685-1111 to request credit report

EXPERIAN
1 (888) 397-3742 to request credit report and fraud investigation

TRANSUNION
1 (800) 680-7289 to request fraud investigation
1 (800) 916-8800 to request credit report

1 (877) FACT-ACT (1-877-322-8228)
Central source for annual free credit reports from all credit reporting agencies

1 (888) 5-OPT-OUT (1-888-567-8688)
To opt-out of pre-approved credit card solicitations

U.S. Postal Office
1 (800) 275-8777 to put a hold on your mail while you are away